نشریه علمی "پدافند الکترونیکی و سایبری"

سال هشتم، شماره ۴، زمستان ۱۳۹۹، ص ۵۲-۴۱

علمی– پژوهشی

گمنامی توزیع‌شده بر پایه زنجیره بلوک تجمعی در شبکه اقتضایی خودرویی

فرید رضازاده [۱]، مهدی آقاصرام [۲*]، کیارش میزانیان [۳]، سیداکبر مصطفوی [۴]

۱- دانشجوی دکتری دانشگاه یزد، ۲- دانشیار دانشگاه یزد، ۳- استادیار دانشگاه یزد، ۴- استادیار دانشگاه یزد

(دریافت: ۱۳۹۸/۰۷/۰۸، پذیرش: ۱۳۹۸/۱۱/۱۲)

چکیده

سربار انبوه و شکست‌های فراوان همبندی، ازجمله چالش‌های گمنام‌سازی در شبکه اقتضایی خودرویی است. از سوی دیگر، زنجیره بلوک با تکیه‌بر خرد، آگاهی و مشارکت جمعی، اقدام به تائید و ارسال تراکنش‌های حاوی اطلاعات می‌کند، به‌گونه‌ای است که افزون بر توانایی ره‌گیری داده‌های تاریخچه‌ای، دارای امتیاز کلیدی دسترس‌پذیری بیشینه است. این امتیاز کلید حل چالش شکست همبندی شبکه و انگیزه بنیادین ارائه این پژوهش است. هرچند سوار کردن فرایند زنجیره بلوک بر شبکه اقتضایی خودرویی، چالش همبندی را حل می‌کند، ولی تأخیر و سربار راه‌اندازی آن، چالش سربار انبوه را تشدید می‌کند. روش پیشنهادی با تجمیع تراکنش‌های خودروهای مختلف در یک بلوک بزرگ، چالش سربار و تأخیر اولیه راه‌اندازی و گمنامی مسیر خودروهای ارسال‌کننده تراکنش را حل کرده و با به‌کارگیری رمزنگاری نامتقارن، گمنامی هویت را برآورده نموده است. برای تجمیع تراکنش‌های خودروهای مختلف، مستلزم تحمل تأخیر زمان تولید و انتشار تعداد زیادی تراکنش جهت تکمیل یک بلوک بزرگ است. این چالش نیز با به‌کارگیری فرایند گره ساختگی و تولید تراکنش‌های ساختگی رفع شده است. از طرف دیگر با گمنام سازی گراف شبکه و به‌کارگیری فرایندهای دوره خاموش و گمنامی k، امنیت تراکنش‌هایی که هنوز تحویل فرایند زنجیره بلوک نشده‌اند را مدیریت می‌کند. شبیه‌سازی روش پیشنهادی ابتدا سناریوهای مختلف شبکه اقتضایی خودروئی را در زیرساخت پایتون ایجاد کرده و سپس معیارهای آن را با سوار کردن زنجیره بلوک معمولی و روش پیشنهادی در آن، مقایسه نموده است. محاسبات احتمال نقض گمنامی با ARX انجام‌شده است. نتایج شبیه‌سازی گویای پایداری روش پیشنهادی، کاهش مطلوب سربار و تأخیر اولیه فرایند در شبکه اقتضایی خودرویی است.

کلیدواژه‌ها: شبکه اقتضایی خودرویی، زنجیره بلوک، امنیت، گمنامی، رمزنگاری

۱- مقدمه

زنجیره بلوک[۱] از جذاب‌ترین کاربردهای رایانش توزیع‌شده در جهان امروز شمرده می‌شود. بخش قابل‌توجه این فناوری، توانایی محاسباتی توزیع‌شده و ذخیره و بازیابی داده بر پایه تراکنش است. امکان رمزنگاری نامتقارن، کاربران را قادر می‌سازد، بدون نیاز به ارائه اطلاعات و شناسه‌های هویتی خود، اقدام به انجام ارتباطات، خریدوفروش و جابه‌جایی پول کنند. تراکنش‌ها در نسخه‌های متعدد، در فضای سخت‌افزاری همگی کاربران، نگهداری می‌شود. ازاین‌رو، شکست‌های پی‌درپی هم‌بندی شبکه، اخلال جدی در دسترسی کاربران به داده‌های توزیع‌شده نمی‌کند؛ بنابراین، پیاده‌سازی چنین سازوکاری در شبکه‌های ناپایدار ازجمله شبکه اقتضایی خودرویی توجیه‌پذیر است.

زنجیره بلوک، یک پایگاه داده توزیع‌شده بر پایه تراکنش است که توسط هم‌اندیشی کاربران گردانده می‌شود. پیامد هر عملیات ویرایش، حذف و ایجاد داده، پدید آمدن یک تراکنش جدید است. درواقع، زنجیره تراکنش‌ها، همچون بایگانی[۲] پایگاه داده، توانایی بازیابی[۳] داده‌های ازدست‌رفته را فراهم می‌کند. این امر با جلو[۴] و عقب‌گرد[۵] کردن تراکنش‌های تاریخچه‌ای انجام می‌شود؛ بنابراین، در غیاب هرگونه کنترل‌کننده مرکزی، یکپارچگی[۶] داده‌ها تأمین‌شده است. هر کاربر، دارای یک رونوشت از همگی تراکنش‌ها است که در درون بلوک‌های دربرگیرنده تراکنش‌های اتمیک[۷]، ذخیره شده‌اند. فراخور با افزونی داده، بلوک جدید ساخته می‌شود. یک کاربر، با به‌کارگیری اثبات کار[۸] به‌عنوان رهبر گزینش‌شده و بلوک جدید را به زنجیره بلوک اضافه می‌کند. سازوکار اثبات کار، به‌سادگی یافتن راه‌حل یک مسئله

* رایانامه نویسنده مسئول: mehdi.sarram@yazd.ac.ir

[1] BlockChain

[2] Log
[3] Recovery
[4] Redo
[5] Undo
[6] Integration
[7] Atomic
[8] Proof of Work

ریاضی است. همانند یافتن مقدار n برای داده x، به‌طوری‌که حاصل افزودن نگاشت هش[1] n به x از مقدار مشخص Y کوچک‌تر باشد.

هر بلوک دارای یک شناسه وراثتی است که توسط توابع هش با به هم پیوستن شناسه بلوک پیشین و داده‌های بلوک کنونی ساخته‌شده است. توابع هش، داده‌هایی با اندازه متفاوت را به‌اندازه ثابت نگاشت می‌کند. از سوی دیگر، دگر گونی محتوی یک بلوک، منجر به تغییر شناسه هش آن خواهد شد. سرانجام، پیوند آن با زنجیره بلوک قطع‌شده و تأییدیه اجماعی کاربران از دست می‌رود. این فرایند، یکپارچگی داده‌ها را پشتیبانی می‌کند.

درروش پیشنهادی، یک تراکنش می‌تواند درخواست جابه‌جایی پول و یا حتی فرستادن یک متن باشد. نخست تراکنش همه پخشی می‌شود. پس از دریافت آن در هر خودرو، به همراه تراکنش‌های دیگر، درون یک بلوک جدید قرارگرفته و پس از دریافت تأییدیه اجماعی به زنجیره بلوک متصل می‌شود. شناسه هش هر بلوک دربرگیرنده اطلاعاتی از همه تراکنش‌های پیشین است. بدین‌سان، با به‌کارگیری شناسه‌های هش، بلوک‌ها به‌صورت پیاپی و زنجیروار به یکدیگر متصل می‌شوند. قابل‌ذکر است، هرگونه دگر گونی در یک بلوک، منجر به تغییر در شناسه هش و گسستن پیوند آن و همگی فرزندانش با زنجیره بلوک می‌شود. برای پیوند مجدد به زنجیره بلوک نیز با اجماع مخالفان روبرو شده و محکوم‌به فنا است. نقطه‌ضعف این روش، ساخت شناسه هش تکراری برای محتوی یکسان است که با به‌کارگیری مقدار تصادفی نانس[2] حل می‌شود. با افزودن مقدار نانس به محتوی یک بلوک، بلوک‌های یکسان، شناسه‌های هش متفاوت خواهند داشت. هر خودرو برای فرستادن تراکنش، نیازمند آدرس اختصاصی دربرگیرنده یک کلید عمومی و یک کلید خصوصی است. شماره شانزده‌رقمی کارت‌بانکی، نمونه خوبی برای کلید عمومی و رمز کارت، یک کلید خصوصی است. تراکنش‌ها با کلید خصوصی خودرو امضاشده، با پیوست شناسه خودرو تکمیل و با کلید عمومی رمز می‌شود. در مقصد با به‌کارگیری کلید عمومی، شناسه خودرو استخراج‌شده، با کلید خصوصی متناظر آن در فهرست مشتریان رمزگشایی خواهد شد. به‌غیراز شناسه هش خودرو، هیچ شناسه هویتی دیگری فرستاده نشده و با توجه به وارون ناپذیری توابع هش، احتمال کشف هویت خودرو وجود ندارد؛ بنابراین، گمنامی هویت به‌درستی تأمین‌شده است.

با رویکرد سربار ترافیکی موردنیاز جهت دریافت تأییدیه اجماعی، روش پیشنهادی اقدام به پدید آوردن بلوک‌های بزرگ، دربرگیرنده شمار زیادی تراکنش از خودروهای مختلف نموده است. در این صورت با رویکرد، بودن چند مقصد در یک بلوک، گمنامی مسیر نیز برآورده گردیده است. از سوی دیگر فرستادن بلوک‌های مجتمع، سربار و تأخیر راه‌اندازی فرایند را به‌شدت کاهش می‌دهد.

پیش از جمع‌آوری تراکنش‌ها در یک بلوک، احتمال شکست حریم خصوصی وجود دارد. ازآنجاکه، تراکنش‌های مالی نیازمند سازوکارهای امنیتی فراگیر است و داد و ستد داده‌های حساس و محرمانه کاربران با شرکت‌های تجاری در ترویج و فروش محصولات، خدمات و مشاوره اجتناب‌ناپذیر است [۱]. همچنین، هیچ‌یک از ذینفعان توان تضمین حریم خصوصی فراگیر کاربران را ندارند. روش پیشنهادی با ناحیه‌بندی خودروها و گمنام‌سازی گراف شبکه هر ناحیه، سعی در کاهش خطرپذیری حریم خصوصی نموده است.

الگوی[3] یک شبکه به‌صورت گراف $G=(V, E, L, \lambda)$ بیان می‌شود. V مجموعه رئوس و مجموعه $E= \{E_1, E_2, \ldots, E_n\}$ نشان‌دهنده یال‌های میانی رئوس گراف، دربرگیرنده انواع پیوندهای میان کاربران شبکه است. λ نگاشت مجموعه برچسب‌های L به رئوس و یال‌های گراف شبکه است.

قبل از انتشار هر پیام، پردازش گراف انجام‌شده و شناسه‌های منحصر به‌فرد کاربر حذف می‌شود. بااین‌همه، مهاجم آگاه، قادر به شکستن حریم خصوصی بدون نیاز به شناسه‌های منحصربه‌فرد است. با رویکرد به وجود دسته‌بندی زیر [۲]، روش پیشنهادی، عمل حذف ویژگی، ایجاد ابهام و اعوجاج درداده را متناسب با هر دسته از ویژگی‌ها، گزینش و به‌کارگیری می‌کند.

- ویژگی‌های کلیدی: تهدید مستقیم این ویژگی در شناسایی منحصربه‌فرد کاربر است. به‌ناچار نیازمند حذف ویژگی است.
- شبه شناسه[4]: آمیختن شبه شناسه‌ها با یکدیگر، منجر به شناسایی و استنتاج ویژگی‌های حساس می‌شود. افزایش درجه گمنامی و مهار شمار پرس‌وجوها، راهکار رویارویی با آن است. درعین‌حال، احتمال استنتاج غیرمستقیم وجود دارد[۳]. از برجسته‌ترین مراحل فرآیند گمنامی، برگزیدن درست گروه شبه شناسه‌ها و گزینش درجه گمنامی است. گمنامی k[5] به معنی ارجاع حداقل k-۱ عضو دیگر با یک‌شبه شناسه است. درجه گمنامی وابستگی مستقیم به چگالی خودروها در یک ناحیه دارد. درصورتی‌که درجه گمنامی برآورده نشود، برای جلوگیری از افشای ویژگی‌های حساس، از به‌کارگیری دوره خاموشی[6]، گره ساختگی[7] و پنهان‌سازی

[1] Hash
[2] Nonce
[3] Model
[4] Semi Identifer
[5] K-Anonymity
[6] Silent Period
[7] Dummy Node

منطقه[1] که مصرف منابع و کاهش بهره شبکه را در پی دارد، یاری گرفته می‌شود [۴-۹].

- ویژگی‌های حساس: آشکار شدن ویژگی حساس از موارد اصلی شکستن حریم خصوصی است. هماهنگ با سنجش حساسیت، عمل حذف ویژگی، ایجاد ابهام و اعوجاج درداده صورت می‌گیرد. انگیزه مهاجمان، حساسیت یک ویژگی را تعیین می‌کند. از سوی دیگر، ویژگی غیر حساس هرگز برای مهاجمان سودمند نخواهد بود.

چالش‌های زیر در گمنام‌سازی متمرکز شبکه اقتضائی خودرویی که طبعاً با به‌کارگیری یک سرور گمنامی انجام می‌شود، مطرح است.

- ✓ مصرف بالای پهنای باند در به‌روزرسانی سرور [۱۰].
- ✓ تحرک خودروها مستلزم به‌روزرسانی دوچندان سرور [۱۱].
- ✓ شکست پیاپی هم‌بندی شبکه و ارتباط ناپایدار با سرور [۱۰].
- ✓ دوگانگی گراف گمنامی با گراف اصلی شبکه [۱۱] و [۱۳].
- ✓ سربار جابه‌جایی پیام‌های کنترلی، بیش از توان شبکه [۱۴].
- ✓ تغییرات پرشتاب و نبود مجال برای اعتمادسازی [۱۳].

از سوی دیگر، ویژگی‌های زنجیره بلوک عبارت‌اند از

- ✓ غیرقابل تغییر بودن
- ✓ مقاوم بودن در برابر هک
- ✓ پایداری داده‌ها حتی پس از گسستن ارتباط مالک تراکنش
- ✓ نبود سرور متمرکز و پایداری در خرابی و شکست هم‌بندی
- ✓ شناسایی یکتای هر بلوک در ساختار سلسله مراتبی

از هم سنجی ویژگی‌های زنجیره بلوک و چالش‌های گمنام‌سازی، نتایج زیر به‌دست می‌آید:

- ✓ بدون تغییر بودن، به معنی حل چالش به‌روزرسانی است.
- ✓ پایداری، حل چالش شکست‌های پیاپی هم‌بندی است.
- ✓ مقاوم در برابر هک یعنی عدم نیاز به گراف و سرور گمنامی
- ✓ شناسایی یکتای هر بلوک جایگزین فرایند اعتمادسازی است.

بنابراین، کاربرد زنجیره بلوک با تدابیر خاص روش پیشنهادی، راهکاری شایسته‌ای برای پیاده‌سازی گمنامی توزیع‌شده در شبکه اقتضایی خودرویی است.

در فصل ۲، نوآوری روش پیشنهادی تشریح شده است. ادبیات پژوهش در فصل ۳، بررسی شده و در فصل ۴، روش پیشنهادی ارائه شده است. در فصل ۵، دستاوردهای پیاده‌سازی روش پیشنهادی با به‌کارگیری پایتون و نرم‌افزار ARX ارائه شده است. در نهایت در فصل ۶، نتیجه‌گیری صورت گرفته است.

[1] Cloaking-Region

۲- نوآوری روش پیشنهادی

در مواردیکه جریان ترافیک یا به عبارت دیگر تعداد خودروهای عبوری در واحد زمان از یک نقطه دلخواه جاده پائین و سرعت خودروها بالا باشد، همبندی شبکه ضعیف بوده و خودروها توانائی ایجاد ارتباط مؤثر و پایدار با یکدیگر را ندارند. سوار کردن فرایند زنجیره بلوک بر شبکه اقتضایی خودرویی، با ذخیره نسخه‌های داده در فضای سخت‌افزاری متعدد کاربران و در نتیجه افزایش دسترسی کاربران به داده‌های توزیع‌شده، قطع دسترسی در شکست‌های پی‌درپی هم‌بندی شبکه را جبران می‌کند. در روش پیشنهادی با افزایش تعداد معدن‌کاوان بلوک[2] به میزان حداقل یک معدن کاو در هر ناحیه، این چالش را پوشش محلی کافی داده است.

صرف به‌کارگیری زنجیره بلوک در الگوی اجماع اثبات کار موجب افزایش گمنامی نمی‌شود. گمنامی هویت مالک تراکنش با رمزنگاری نامتقارن برآورده شده است [۱۵]. از سوی دیگر، تجمیع تراکنش‌های خودروهای مختلف در یک بلوک، تأمین‌کننده گمنامی مسیر است.

الگوهای اجماع بر پایه اثبات کار، نیازمند صرف زمان زیادی برای رسیدن به توافق است و نصب زنجیره بلوک در شبکه خودرویی مخاطره‌آمیز است و می‌تواند باعث متوقف شدن شبکه شود؛ بنابراین، چالاکی و پایداری فرایند زنجیره بلوک نصب‌شده در شبکه اقتضائی خودروئی، نقطه کلیدی روش پیشنهادی است. به‌طوری‌که با افزایش زمان شبیه‌سازی و طول جاده و تعداد خودرو سازوکار مصرف پهنای باند حدود ۵۰ درصد باقی‌مانده و تأخیر یک پرش نیز قابل قبول و شبکه کاملاً پایدار است. از طرف دیگر روش پیشنهادی تأخیر راه‌اندازی فرایند زنجیره بلوک را ۸۰ درصد کاهش داده است. با طراحی الگوی ترافیکی و برگزیدن مسیریابی اپیدمی، چالش پایداری و با تولید بلوک‌های مجتمع، چالش تأخیر راه‌اندازی فرایند حل شده است. از سوی دیگر، با به‌کارگیری نودها و تراکنش‌های مجازی، زمان انتظار برای تولید تعداد تراکنش موردنیاز برای تکمیل گنجایش یک بلوک تعدیل شده است. همچنین، توانایی تنظیم مقادیر آستانه‌ای و هماهنگ با ضرورت ارسال پیام، فراهم گردیده است.

انگیزه خودروها برای مصرف منابع خود در بررسی بلوک‌ها، بر پایه کارمزد تراکنش‌های مالی برآورده می‌شود. با رویکرد وجود نود و تراکنش‌های، تراز کارمزد بلوک‌های مختلف یکسان نیست. از سوی دیگر، نباید با مقایسه کارمزد بلوک‌ها، مقدار درصد تراکنش‌های واقعی هر بلوک استنتاج شود. شایان ذکر است، کوچک بودن درصد تراکنش‌های واقعی در یک بلوک، می‌تواند

[2] Block Miner

منجر به کشف مسیر تراکنش‌ها گردد [۱۶]؛ بنابراین، در مقصد، کارمزد تراکنش‌های موفق محاسبه و پرداخت می‌گردد.

پیش از جمع‌آوری تراکنش‌ها در یک بلوک، پردازش گراف انجام شده و از حذف ویژگی، ایجاد ابهام و اعوجاج، هماهنگ با ویژگی‌های هر خودرو استفاده شده است.

۳- کارهای مرتبط

در سال ۱۹۷۹ درخت هش رالف مرکل نوآفرینی شد. کاربرد آغازین درخت هش در امضای لم پورت و رمزنگاری بود [۱۷]. در سال ۱۹۹۱ پژوهشگران رمزنگاری، برای نخستین بار از زنجیره بلوک در پشتیبانی اعتبار اسناد استفاده کردند [۱۸]. برتری روش: توانایی پشتیبانی زمان تولد و ویرایش اسناد، مالکیت اسناد، به‌کارگیری سرور علامت‌گذاری زمانی[1] و توانایی ره‌گیری تغییرات اسناد است. نقطه‌ضعف روش: احتمال شکست حریم خصوصی مالکان اسناد و همچنین آسیب دیدن اسناد، در هنگام جابه‌جایی سرور علامت‌گذاری زمانی است.

در سال ۱۹۹۳، با به‌کارگیری توابع هش، محتویات سند، نخستین شناسه منحصربه‌فرد تولید شد [۱۹]. با هر تغییر در متن یک سند، شناسه هش متفاوتی ساخته می‌شد. از آمیختن این ایده با امضای دیجیتال، تنها شناسه هش به سرور علامت‌گذاری زمانی ارسال شد [۲۰] بدین‌سان، ایده بنیادین زنجیره بلوک پا به میدان پژوهش گذاشت.

در سال ۲۰۰۸ ساتوشی ناکاموتو، سازوکار پول دیجیتال را با رویکرد یکپارچگی توزیع‌شده، ارائه و بیت کوین[2] نامید [۲۱].

در سال ۲۰۱۶، زنجیره بلوک در سه عنوان تعریف شد:

زنجیره بلوک: دربرگیرنده بلوک‌هایی که به چینش زمان تولید به‌صورت خطی و زنجیروار به یکدیگر متصل شده‌اند. در واقع با این روش حافظ مسائل امنیتی است. بلوک‌های جدید همیشه به‌صورت خطی و با زمان‌بندی ذخیره و همیشه به زنجیره اضافه می‌شوند. این بدان معنی است که ارتفاع زنجیره بلوک‌ها به صدها هزار بلوک خواهد رسید. پس از اینکه یک بلوک به انتهای زنجیره اضافه شود، به عقب برگشتن و تغییر محتویات بلوک با توجه به وجود شناسه هش آن‌که البته وابسته به شناسه هش بلوک قبلی است، بسیار دشوار است.

تراکنش[3]: هر بلوک دربرگیرنده تراکنش‌های کاربران مختلف است که تنها ازنظر اندازه مشابه‌اند.

معدن‌کاوی: به دریافت تأییدیه اجماعی با محاسبه توابع تصدیق کار[4] (یک سازوکار رأی‌گیری امن و توزیع‌شده مطمئن [۲۲ و ۲۳]، ساخت بلوک جدید و الحاق به زنجیره بلوک، معدن‌کاوی گفته می‌شود. شناسه هش هر بلوک وابسته به بلوک‌های پیشین خود است؛ برای حمله مهاجمان به یک بلوک، نیازمند پردازش همه بلوک‌های پیشین است که در عمل شُدنی نیست.

بنجامینت و همکاران [۲۴] خدمات ایمنی، مالی و اطلاع‌رسانی را با به‌کارگیری زنجیره بلوک در شبکه اقتضایی خودرویی مطرح کردند. پشت‌گرمی روش ارائه شده بر وجود و کاربردی بودن RSU[5] استوار شده است. در بسیاری از محیط‌های شبکه اقتضایی خودرویی امکان وجود RSU در سرتاسر مسیر وجود ندارد. از سوی دیگر، چالش‌های بنیادین مسیریابی و از دست رفتن داده‌ها در شکست‌های پیاپی هم‌بندی شبکه، در نظر گرفته نشده است.

دری و همکاران [۲۵] یک LSB[6] محلی ارائه کردند. با خوشه‌بندی و نصب فرایند زنجیره بلوک در سرخوشه‌ها حریم خصوصی خودرو را پشتیبانی کرده است. نقطه‌ضعف روش، حفظ امنیت سرخوشه است. اگر مهاجم کنترل سرخوشه را به‌دست گیرد، فرایند دچار بحران خواهد شد.

شان روون و همکاران [۲۶] گمنامی هویت خودروها را با به‌کارگیری کلید نامتقارن رمزنگاری، برآورده کردند. برای پایداری زنجیره بلوک در شبکه اقتضایی خودرویی از کانال‌های اولتراسونیک[7] و نوری استفاده شده است [۲۷]. در دو روش بالا، هرچند حریم خصوصی خودرو در ارتباط با مراکز تجاری تضمین‌شده، ولی ارتباط خودرو به خودرو، خارج از فرایند زنجیره بلوک انجام می‌شود، که مستعد نقض حریم خصوصی است.

ژائوجان و همکاران [۱۵]، توانایی برقراری ارتباط میان میلیون‌ها خودرو، با سربار ذخیره‌سازی در حد مگابایت و تأخیر کسری از میلی‌ثانیه را فراهم کردند. با شبیه‌سازی پایتون، فرایند زنجیره بلوک در شبکه اقتضائی خودرویی پیاده‌سازی شده است. پشت‌گرمی روش بر وجود RSU استوار شده است که در بسیاری از محیط‌های شبکه اقتضائی خودرویی کاربرد ندارد. هرچند محاسبات سمت خودرو و همچنین ارتباط خودرو با خودرو کاهش می‌یابد [۲۸].

لی لون و همکاران [۲۹] تأخیر در دریافت تائیدیهِ اجماعی را با تعداد عضو فرایند زنجیره بلوک مرتبط دانسته است. مقدار آستانه‌ای حداقل تعداد خودرو برابر دویست خودرو تعیین شده و اگر شمار خودرو بیش از شش‌صد خودرو باشد، تأخیر بسیار اندک و بازده شبکه بهتر از حالت عادی است.

[1] Time Stamp
[2] BitCoin
[3] Transaction
[4] Proof-of-Work (PoW)
[5] Road-Side-Unit
[6] Lightweight Scalable Blockchain
[7] Ultrasonic

یوان و همکاران [۳۰] الگوی تنوع ۱ را با درجه k برای حفاظت از اطلاعات ساختاری و ویژگی‌های حساس کاربران تعریف کردند. به‌طورکلی گمنامی k تضمین می‌کند که اطلاعات هر کاربر، نمی‌تواند از حداقل k-۱ کاربر دیگر قابل‌تشخیص باشد [۳۱]. یک کاربر تنوع ۱ دارد، اگر و فقط اگر، حداقل ۱ جانشین برای ویژگی‌های حساس کاربر وجود داشته باشد [۳۲].

روش‌های تأمین امنیت در شبکه اقتضایی خودرویی با مشکل شکست‌های مکرر هم‌بندی شبکه مواجه‌اند. حل این چالش به طرق مختلف و با استفاده از RSU [۱۵]، [۲۵] و [۲۹]، خوشه‌بندی و مدیریت نیمه‌متمرکز در سرخوشه‌ها [۲۵]، کانال اولتراسونیک و نوری [۲۶]، بررسی و حل نموده‌اند و یا به‌طورکلی چالش‌های مسیریابی و از دست رفتن داده‌ها در شکست‌های پیاپی هم‌بندی شبکه خودرویی را بررسی نکرده و صرفاً به نحوه نصب و تنظیم زنجیره بلوک پرداخته‌اند. در محیط‌های معمول شبکه اقتضایی خودرویی، پوشش سرتاسری RSU، کانال اولتراسونیک، و نوری امکان‌پذیر نیست. از سوی دیگر، حفظ امنیت سرخوشه، نقطه بحرانی استفاده از خوشه‌بندی و انتخاب خودرو مناسب برای مدیریت نیمه‌متمرکز است، چراکه، اگر مهاجم کنترل سرخوشه را به‌دست گیرد، امنیت فرایند دچار بحران جدی خواهد شد. درروش پیشنهادی با پیاده‌سازی زنجیره بلوک و ذخیره کامل بلوک‌های آن در تک‌تک خودروهای ناحیه‌بندی شده، چالش از دست رفتن داده‌ها، در شکست‌های مکرر هم‌بندی حل شده و حاصل آن پایداری شبکه در طی زمان است، به‌طوری‌که برای تعداد ۱۶۰۰ خودرو سازوکار مصرف پهنای باند ۵۵ درصد و تأخیر یک پرش به ۰/۶ میلی‌ثانیه کاهش‌یافته است. با تغییر سناریوی شبیه‌سازی و افزایش زمان شبیه‌سازی از ۱۲۰۰ ثانیه به ۳۰۰۰ ثانیه و افزایش طول جاده از ۴ کیلومتر به ۲۰ کیلومتر، برای تعداد ۲۲۵۰ خودرو، مصرف بیشینه پهنای باند ۴۰ درصد و تأخیر یک پرش به میانگین ۳ میلی‌ثانیه افزایش‌یافته است و شبکه هنوز کاملاً پایدار است. از طرف دیگر روش پیشنهادی تأخیر راه‌اندازی فرایند زنجیره بلوک را ۸۰ درصد کاهش داده است.

جدول (۱): مقایسه روش پیشنهادی با ادبیات تحقیق

مرجع	روش تأمین هم‌بندی شبکه	مزیت	تعداد خودرو	سازوکار مصرف پهنای باند	تأخیرMs	UnlinkAbility
۱۵	استفاده از RSU	تأخیر قابل قبول	۱۰۰k	-	۰,۴۴۲	Ring Pair
۲۵	استفاده از RSU و خوشه‌بندی	بهبود زمان تأخیر اثبات کار	-	-	کاهش۴۰٪	Ring Public Key
۲۶	استفاده از کانال‌های با برد بالا	افزایش مسافت تبادل پیام	-	-	-	identity salt
۲۹	استفاده از RSU	پایداری شبکه در زمان	۱۰۰۰	-	۴۵,۵۷	Ring Pair
روش پیشنهادی	ناحیه‌بندی و بلوک‌های بزرگ	پایداری شبکه در زمان	۲۲۵۰	٪۵۵	۰,۶	Ring Pair

۴- روش پیشنهادی

در این بخش الگوریتم روش پیشنهادی باهدف حل چالش‌های گمنام‌سازی در شبکه اقتضایی خودرویی ارائه شده است.

بر پایه بردار ویژگی ذخیره‌شده در جداول مسیریابی، همسان‌ترین خودروها برای سازمان‌دهی نواحی شباهت گزینش و فهرست خودروهای همسایه، دربرگیرنده اعضای یک ناحیه تشکیل می‌شود.

بردار ویژگی از ویژگی‌های اصلی الگوی ترافیک شبکه شامل: سرعت، جهت و مختصات طولی جاده و به همراه اندازه صف پیام‌های خروجی هر خودرو تشکیل شده است. با رویکرد، قابل‌اغماض بودن زمان پردازش گراف شبکه یک و با تمرکز برگراف گمنامی یک ناحیه، پیش از فرستادن هر تراکنش، الگوریتم زیر در خودروهای ارسال‌کننده اجرا می‌شود.

سازمان دادن ناحیه شباهت با رویکرد الگوی ترافیک شبکه:

- ✓ ساخت گراف گمنامی ناحیه‌ای که ارسال از آن آغاز می‌شود
- ✓ زدایش مقادیر منحصربه‌فرد رأس‌های گراف گمنامی ناحیه
- ✓ زدودن یال‌های حساس گراف گمنامی ناحیه
- ✓ ساخت فهرست همسایه‌ها از خودروهای بجای مانده در گراف
- ✓ مقدار k (معیار گمنامی) توسط هر خودرو مشخص می‌شود.
- ✓ اگر مقدار k بزرگ‌تر از شمار خودروهای ناحیه شباهت بود، خودرو وارد دوره خاموشی می‌شود.
- ✓ اگر زمان دوره خاموشی از مرز آستانه‌ای مشخص، بیشتر شد، از روش گره ساختگی به میزان تفاضل k و شمار خودروهای ناحیه شباهت، خودرو مجازی ساخته و به فهرست همسایه‌ها و گراف گمنامی اضافه می‌شود.

- ✓ اگر اندازه k کوچک‌تر یا برابر شمار خودروهای ناحیه شباهت باشد، تراکنش با به‌کارگیری رمزنگاری نامتقارن، مطابق با رابطه (۳) رمزنگاری شده و همه پخشی می‌شود.

هر خودرو در زمان دریافت، الگوریتم زیر را اجرا می‌کند.

- ✓ تراکنش دریافتی به استخر[1] تراکنش‌های خودرو اضافه می‌شود [۳۳].
- ✓ اگر اندازه استخر تراکنش به‌اندازه مشخص‌شده یک بلوک رسید، بلوک جدید تولید شده و برای کسب تأییدیه اجماعی، همه پخشی می‌شود. پس از دریافت تأییدیه اجماعی بلوک جدید دربرگیرنده چندین تراکنش، یک برچسب زمانی و شناسه به‌دست‌آمده از آمیختن هش بلوک‌های پیشین، به زنجیره بلوک الحاق می‌گردد. روال عملکرد در شکل (۲) توصیف شده است. درواقع هر خودرو افزون بر در اختیار داشتن کلید خصوصی خود و کلید عمومی مقصدهای معتبر، نقش معدن‌کاوی بلوک را بازی کرده و ناگزیر به رعایت شرایط و قوانین توابع تصدیق کار است.

با به‌کارگیری رابطه (۱)، فاصله بردار ویژگی دو خودرو محاسبه و ناحیه‌بندی بر پایه آن انجام می‌شود، d فاصله بین خودروهای V_i و V_j، x_{i_l} ویژگی l ام از بین m ویژگی خودرو V_i و x_{j_l} ویژگی l ام از بین m ویژگی خودرو V_j است.

$$d(V_i, V_j) = \sum_{l=1}^{m} |x_{i_l} - x_{j_l}| \qquad (۱)$$

با به‌کارگیری رابطه (۲)، بردار ویژگی خودروهای، از میانگین بردارهای ویژگی همه خودروهای ناحیه نگاشت می‌شود؛ درنتیجه، دو خودرو مجازی که هم‌زمان تولید می‌شوند، بردار ویژگی یکسان نخواهند داشت. x_{*_l} ویژگی l ام از یک خودرو مجازی، n تعداد عضو ناحیه شباهت و x_{i_l} ویژگی l ام از خودرو i ام در ناحیه شباهت است.

$$x_{*_l} = \frac{\sum_{i=1}^{n} x_{i_l}}{n} \qquad (۲)$$

در تبادل جداول مسیریابی، هر خودرو به بردار ویژگی خودروهای همسایه دسترسی دارد. بدین‌سان، افزون بر ناحیه‌بندی درست‌تر، هر خودرو درجه گمنامی خود را درست‌تر تعریف خواهد کرد.

[1] Pool

این الگوریتم در شبه‌کد زیر ارائه شده است.

Algorithm1: K-Anonymity Method

Input: R.ks, R.featurevetor
R Requester which has a message to send
Ka k_Anonymity state
Sm Silence mode state
R.Ks Scaler Value For K-Anonymity
T_1 Maximum Time Of Silene Mode
NL neighbor list
Sc silence counter
Set feature vectore = $\{f_j\}0<j<m+1$
Set Oponlist = $\{o_i\}0<i<n+1$ Open List of avaleable vehicles for R
Set Closedlist = $\{c_i\}0<i<k+1$ Close List of similar vehiles corespond for anonymizing R

1. k = R.ks
2. Ka = false
3. For i:= 1 To n Do
4. Begin
5. If distane(R.featurevetor,o_i.featurevetor) is less than L_1 and same direction, near location and speed
6. Then Closedlist = Closedlist+o_i
7. End
8. Create G = (V,E) with Closedlist $v_i = o_i$ & make relation with connecting $v_i.f_j$ to $o_i.f_j$
9. Delete □ v_i where is mutual exclusive
10. Delete □ $v_i.f_j$ to $o_i.f_j$ connection where is sencitive
11. Create NL from □ v_i Є G
12. If Sc > T_1 Then
13. While k > count(NL.v_i) do
14. Add dummy node to NL & G and add Dummy link to some v_i Є NL & G
15. Set R.Sm to false
16. Set R.Ka to true
17. Sc = 0
18. Else
19. Sc = Sc + 1
20. Set R.Sm to true
21. Set R.Ka to false
22. Create a transaction for the message
23. Broadcast the transaction

Output K Input Value For K-Anonymity Method

چنانچه در شبه‌کد ۱ مشاهده می‌شود، با به‌کارگیری فرایندهای پردازش گراف، دوره خاموش، گره ساختگی و پنهان‌سازی منطقه، حریم خصوصی دارندگان تراکنش، پیش از الحاق به زنجیره بلوک مدیریت شده است.

روال ایجاد و اتصال یک بلوک جدید به زنجیره بلوک در شبه‌کد ۲ ارائه شده است.

Algorithm2: Mining a Block

Input: Index, Previoushash, Timestamp, Data, Hash, Nonce
If (PreviousBlock.Index + 1 == NextBlock.Index) And
(PreviousBlock.Hash == NextBlock.PreviousHash) And
(NextBlockHash == NextBlock.Hash) And
IsValidHashDifficulty(NextBlockBash)) Then
Begin
Hash(Index, Previoushash, Timestamp, Transactions, Nonce);
GenerateNextBlock(Data);
ADDBlock(Index, Previoushash, Timestamp, Data, Hash, Nonce);
End
Output ADD a New Block to BlockChain

ساختار یک بلوک مطابق با جدول (۱) پیکربندی می‌شود.

جدول (۱): ساختار یک بلوک

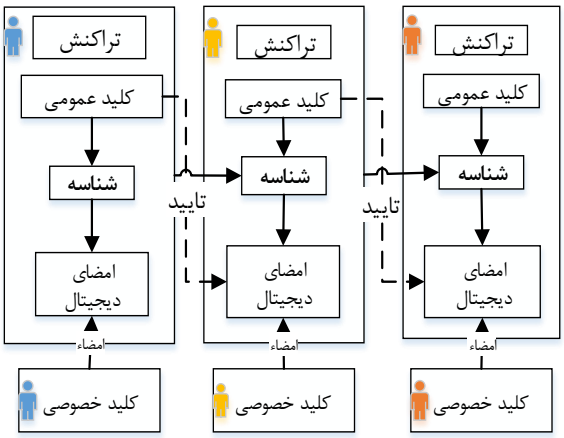
نام فیلد	نوع فیلد	سایز
تمبر زمانی	time	24 bit
تراکنش	Array of string	متغیر
نانس	byte	8 bit
هش بلوک قبلی	bit	32 bit
هش بلوک فعلی	bit	32 bit

ساختار یک تراکنش مطابق با جدول (۲) پیکربندی می‌شود.

جدول (۲): ساختار یک تراکنش

نام فیلد	نوع فیلد	سایز
تمبر زمانی	time	8 bit
متن	string	متغیر
کلید عمومی مقصد	bit	32 bit
کلید عمومی مقصد	bit	32 bit

نخست با به‌کارگیری وراثت شناسه هش، بلوک جدید تأیید شده و سپس شناسه هش جدید که از بلوک‌های والد، برچسب زمانی، محتوی بلوک جدید و مقدار نانس ساخته می‌شود، به آن تخصیص می‌دهد. این شناسه افزون بر منحصربه‌فرد بودن، متصل‌کننده بلوک جدید به بلوک‌های پیشین است. معماری و نحوه امضای هر تراکنش در شکل (۱) ارائه شده است.



شکل (۱): معماری تراکنش

هر دو کلید خصوصی و عمومی، از فرمت کیف پول (WIF) و از هم‌آمیزی حروف و اعداد بسیار طولانی تشکیل شده است. در رابطه رمزنگاری نامتقارن ۳، T_s تراکنش در حال تولید، S شناسه ارسال‌کننده، PU_r کلید عمومی مقصد، C پیام رمز شده و PR_s کلید خصوصی ارسال‌کننده است.

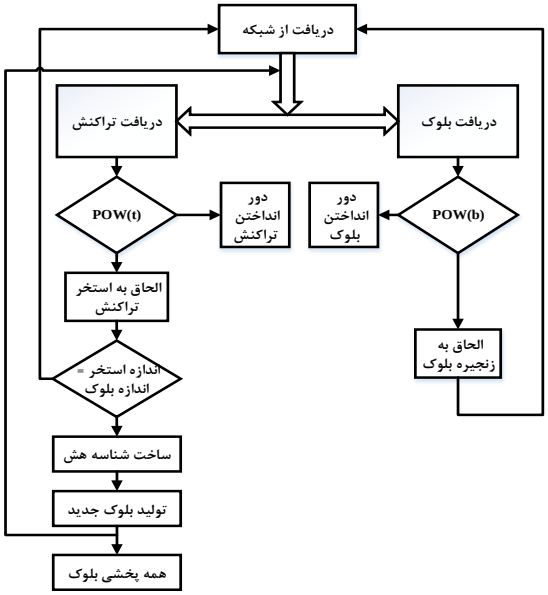
$$C = E\left(PU_r, \left(s, E(PR_s, T_s)\right)\right) \quad (۳)$$

در مقصد، برای کشف رمز شناسه ارسال‌کننده، از رابطه (۴) استفاده می‌شود. کلید خصوصی ارسال‌کننده از تطبیق شناسه وی با فهرست، به‌دست‌آمده و از رابطه ۵ متن تراکنش رمزگشایی خواهد شد.

$$s = D(PU_r, C) \quad (۴)$$

$$T_s = D\left(\mathrm{PU_r}, \left(\mathrm{D(PR_s, C)}\right)\right) \quad (۵)$$

اگر شمار بلوک‌های والد یک بلوک جدید بیش از یک‌دوم کل خودروهای تأییدکننده باشد، رأی اکثریت حاصل خواهد شد و اگر بیش از دوسوم باشد، دارای رأی اکثریت قاطع خواهد بود. نحوه عملکرد هر خودرو در شکل (۲) توصیف شده است.



شکل (۲): نحوه اجرای الگوریتم در هر خودرو

در مرور ادبیات تحقیق، روش‌های تأمین امنیت در شبکه اقتضایی خودرویی با مشکل شکست‌های مکرر هم‌بندی شبکه مواجه‌اند. حل این چالش به طرق مختلف و با استفاده از RSU [۱۵] و [۲۵]، خوشه‌بندی و مدیریت نیمه‌متمرکز در سرخوشه‌ها [۲۶]، کانال اولتراسونیک و نوری [۱۵] و [۲۷]، بررسی و حل نموده‌اند و یا به‌طورکلی چالش‌های مسیریابی و از دست رفتن داده‌ها در شکست‌های پیاپی هم‌بندی شبکه خودرویی را بررسی نکرده و صرفاً به نحوه نصب و تنظیم زنجیره بلوک پرداخته‌اند. در محیط‌های معمول شبکه اقتضایی خودرویی، پوشش سرتاسری RSU، کانال اولتراسونیک، و نوری امکان‌پذیر نیست. از سوی دیگر، حفظ امنیت سرخوشه، نقطه بحرانی استفاده از خوشه‌بندی و انتخاب خودرو مناسب برای مدیریت نیمه‌متمرکز است، چراکه، اگر مهاجم کنترل سرخوشه را به‌دست گیرد، امنیت فرایند دچار بحران جدی خواهد شد. درروش پیشنهادی با پیاده‌سازی زنجیره بلوک و ذخیره کامل بلوک‌های آن در تک‌تک خودروهای ناحیه‌بندی شده، چالش از دست رفتن داده‌ها، در شکست‌های مکرر هم‌بندی حل شده است.

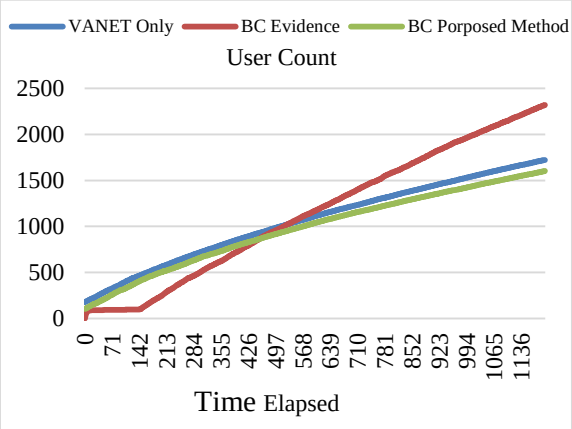
۵- نتایج شبیه‌سازی

در شبیه‌سازی انجام شده با به‌کارگیری پایتون، چگونگی عملکرد زنجیره بلوک در شبکه اقتضایی خودرویی ارزیابی شده است. پیکربندی متغیر، موجب شکست‌های پی‌درپی هم‌بندی شبکه خواهد شد؛ بنابراین، پایداری یک مسیر پایان به پایان دست نایافتنی است. برای رویارویی با این چالش، از ارتباط گام‌به‌گام به‌جای پایان به پایان استفاده می‌شود.

در این پیاده‌سازی از مسیریابی اپیدمی استفاده شده است. امتیاز اصلی مسیریابی اپیدمی، انتشار مطمئن پیام در شبکه‌های اقتضایی خودروئی است. الگوی ترافیک، با به‌کارگیری توزیع‌های گوناگون سرعت و مسافت بین خودرویی و بر پایه الگوی IDM[1] و سناریوهای ترافیکی معمول تنظیم شده است. پارامترهای پیش‌فرض الگوی ترافیک با رویکرد ادبیات تحقیق، تنظیم شده است. طول جاده ۲۰ کیلومتر با ۳ باند در هر دو جهت، طول خودروها ۵ متر، تأخیر در هر پرش ۱۰ میلی‌ثانیه از پارامترهای ثابت و سرعت هر خودرو یک متغیر تصادفی است که از الگوی ترافیک در هر ثانیه محاسبه شده و بر اساس سرعت خودروها محل هر خودرو در جاده مشخص می‌گردد. خودروها با مدیریت یک پرچم دو حالتِ اقدام به ارسال تراکنش می‌کنند. هر خودرو قبل از ارسال ناحیه شباهت خود را بر مبنای سرعت، محل و جهت حرکت خودروهای دیگر تشکیل می‌دهد. اگر تعداد خودروهای ناحیه شباهت از ۱۰ خودرو کمتر باشد برای ارسال تراکنش صبر خواهد کرد. در صورتی‌که هر خودرو پیامی با عمر بیش از ۳ ثانیه در استخر خود داشته باشد، اقدام به تولید خودرو مجازی خواهد کرد تا ناحیه شباهت دارای حداقل ۱۰ خودرو باشد. تمامی خودروهای موجود در شعاع ۱۰۰ متری تراکنش را دریافت و به استخر تراکنش‌های خود اضافه می‌کنند. هرگاه استخر هر خودرو دارای بیش از ۱۰ تراکنش رسید یک بلوک جدید تولید و با اخذ تأییدیه اجماعی آن را به زنجیره بلوک اضافه می‌کند. در صورتی‌که هر خودرو پیامی با عمر بیش از ۳ ثانیه در استخر خود داشته باشد، اقدام به ساخت تراکنش مجازی خواهد کرد. شبیه‌سازی در طی ۱۲۰۰ ثانیه انجام و نتایج آن با استفاده از نمودارهای منتج از شبیه‌سازی تحلیل شده است.

در شکل (۳)، نرخ پذیرش خودروها در شبکه اقتضائی خودرویی بدون فرایند زنجیره بلوک، با زنجیره بلوک معمولی و روش پیشنهادی مقایسه شده است. در شبکه اقتضائی خودروئی با زنجیره بلوک معمولی، پذیرش خودروهای جدید، با تأخیر زیاد، همراه است. با رویکرد شرایط اضطرار در این نوع شبکه قابل پذیرفتن نیست.

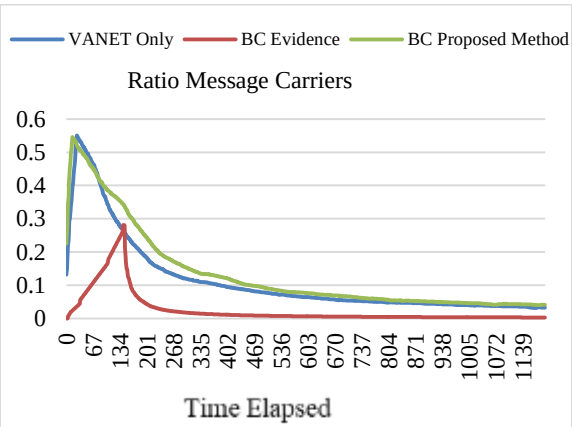
[1] Intelligent_Driver_Model



شکل (۳): نرخ افزایش خودرو در زمان

پذیرش خودروهای جدید در شبکه اقتضائی خودروئی بدون زنجیره بلوک و روش پیشنهادی با نرخ خطی مطلوب، صورت می‌گیرد. چالش اصلی حل‌شده این پژوهش، تأخیر زمانی عضوگیری در آغاز فرایند زنجیره بلوک است.

در شکل (۴)، نرخ انتقال موفق در شبکه اقتضائی خودرویی بدون فرایند زنجیره بلوک، با زنجیره بلوک معمولی و روش پیشنهادی مقایسه شده است. در شبکه اقتضائی خودروئی با زنجیره بلوک معمولی، شاهد رشد اندک اولیه نرخ انتقال موفق و سپس افت شدید و رسیدن به آستانه صفر است.



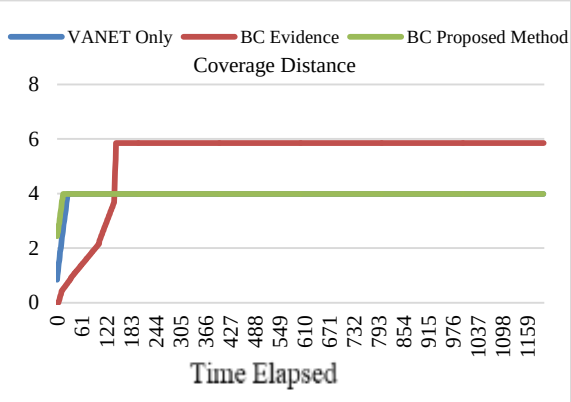
شکل (۴): نرخ انتقال موفق در زمان

درعین‌حال، عملکرد روش پیشنهادی، همانند شبکه اقتضائی خودروئی بدون زنجیره بلوک است. در بیشتر موارد نرخ انتقال موفق بهتری برآورده شده است.

روند پرشتاب رشد و سپس کاهش شدید نرخ انتقال موفق، از روی سرریز شدن صفوف تراکنش‌های دریافتی است. افزایش منابع سخت‌افزاری یکی از راه‌کارهای حل این چالش است. درعین‌حال، از چالش‌های شایان‌ذکر، در شبکه اقتضائی خودرویی پایداری هم‌بندی و انتقال مطمئن پیام است؛ بنابراین، با رویکرد ادبیات پژوهش ژائوجان و همکاران و هم سنجی دستاوردهای

شبیه‌سازی ارائه شده، توانائی زنجیره بلوک در جبران شکست‌های پیاپی هم‌بندی آشکار است.

در شکل (۵)، سنجش مسافت تحت پوشش فرایند، در شبکه اقتضائی خودرویی بدون فرایند زنجیره بلوک، با زنجیره بلوک معمولی و روش پیشنهادی مقایسه شده است. در شبکه اقتضائی خودروئی با زنجیره بلوک معمولی، تأخیر زیاد اولیه، دررسیدن به سقف نهائی پوشش مشاهده می‌شود.



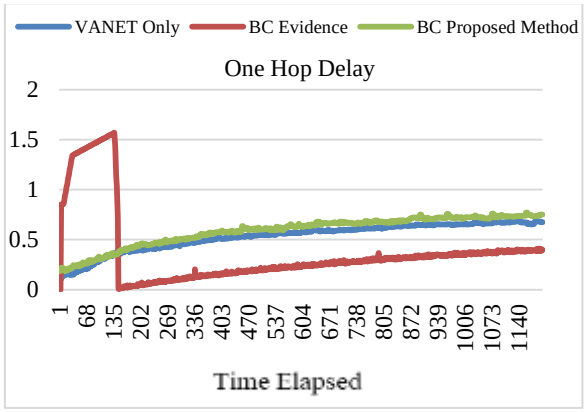
شکل (۵). پوشش مسافت در زمان

از سوی دیگر، با رویکرد ایجاد پوشش مازاد ۵۰ درصدی، نسبت به طول جاده، چالش‌های مصرف منابع اضافی، احتمال نشت اطلاعات و نقض اصل تخصیص حداقل مجوزها وجود دارد.

درعین‌حال، عملکرد روش پیشنهادی همانند شبکه اقتضائی خودروئی بدون زنجیره بلوک بوده و در رشد اولیه مسافت بیشتری را تحت پوشش قرار داده است.

برقراری امنیت فرایند زنجیره بلوک، نیازمند سطح وسیعی از ارتباط نظیر به نظیر[1] بین خودروها است. همچنین این ارتباط باید به ازای هر بلوک در شبکه برقرار شود. تأخیر و سربار مخابراتی زیاد ناشی از این امر و فرایند اجماع اثبات کار، چالشی جدی در شبکه اقتضائی خودرویی محسوب می‌شود. روش پیشنهادی با تشکیل ناحیه شباهت از خودروهای هم سرعت و نزدیک یکدیگر، سعی در سازوکار کردن ارتباط نظیر به نظیر، بین خودروهای هر ناحیه نموده است. با توجه به تشکیل ناحیه‌های متعدد در طول مسیر و وجود خودروهای مشترک در فضای همپوشان ناحیه‌ها، امکان پوشش سرتاسری جاده فراهم و به ازای هر بلوک در شبکه برقرار می‌شود. این مهم در شکل (۵) بررسی و استنتاج شده است. از طرف دیگر، تأخیر و سربار مخابراتی زیادی که درروش متداول زنجیره بلوک به شبکه وارد می‌شود، با تولید بلوک‌های مجتمع، متناسب با اندازه بلوک کاهش‌یافته است و با به‌کارگیری نودها و تراکنش‌های مجازی، زمان انتظار برای تولید تعداد تراکنش موردنیاز برای تکمیل گنجایش یک بلوک تعدیل شده است.

در شکل (۶)، تأخیر میانگین یک گام در شبکه اقتضائی خودرویی بدون فرایند زنجیره بلوک، با زنجیره بلوک معمولی و روش پیشنهادی مقایسه شده است. در شبکه اقتضائی خودروئی با زنجیره بلوک معمولی، تأخیر زیاد اولیه مشاهده می‌شود. افزایش بازده در برابر افزایش شمار خودروها، بسته به عدم نیاز به‌روزرسانی در فرایند زنجیره بلوک و همچنین توزیع فراگیر کل داده‌ها در همه فضای شبکه است. بااین‌همه، با رویکرد وقوع اضطرار دررسیدن بی‌درنگ پیام، تأخیر اولیه فوق، چالشی جدی شمرده می‌شود.



شکل (۶): تأخیر میانگین یک گام با زنجیره بلوک

درعین‌حال، عملکرد روش پیشنهادی همانند شبکه اقتضائی خودروئی بدون زنجیره بلوک است.

با رویکرد چهار مقایسه انجام‌شده، فرایند زنجیره بلوک نصب‌شده بر روی شبکه اقتضایی خودرویی پایدار و کارآمد است. روش پیشنهادی افزون بر حل چالش‌های کارایی زنجیره بلوک معمولی، با تأمین گمنامی هویت و مسیر، چالش‌های بنیادین گمنام‌سازی شبکه اقتضایی خودرویی را نیز حل کرده است. در شکل ۶، شاهد حذف تأخیر راه‌اندازی زنجیره بلوک و در شکل (۴)، ناظر بر آزادسازی پایدار پهنای باند شبکه در ازای افزایش خطی خودروهای درگیر در فرایند هستیم. بنابراین، کارائی و پایداری فرایند تأمین شده است.

با این‌همه، هرچند پس از تحویل هر تراکنش به زنجیره بلوک گمنامی هویت و مسیر فراهم است. احتمال شکست حریم خصوصی پیش از تجمیع تراکنش‌ها در یک بلوک وجود دارد. این چالش نیازمند فرایند ناحیه‌بندی، پردازش گراف هر ناحیه و گمنام‌سازی آن، پیش از فرستادن تراکنش است. تجزیه‌وتحلیل خطرپذیری گمنامی، به‌وسیله بسته نرم‌افزاری ARX انجام شده است.

[1] Peer To Peer

در پیوند زیر، پایگاه داده‌ای، با ۹ ویژگی توصیفی و ۳ ویژگی حرکتی از ۳۹۴ خودروی متفاوت، ارائه شده است.

https://eric.univ-lyon.fr/~ricco/tanagra/fichiers/cars.xls

از معیار خطرپذیری افشای حریم خصوصی و فرض توزیع نرمال ویژگی‌های ترافیکی، در پیاده‌سازی الگوریتم گمنام‌سازی استفاده شده است.

خطرپذیری افشای حریم خصوصی دربرگیرنده سه سناریوی زیر است:

- ✓ تعقیب‌کننده[1]

خطرپذیری شناسایی یک شخص خاص، در یک پایگاه داده برآورد می‌شود.

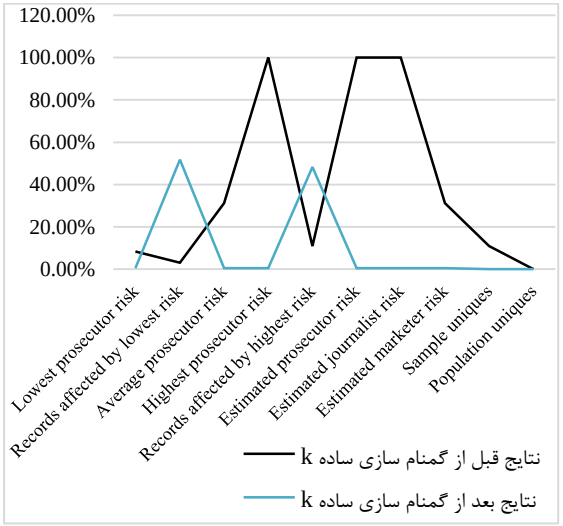
- ✓ خطرپذیری ژورنالیست[2]

بجای شناسایی یک کاربر خاص، بادانش وجود همه کاربران در پایگاه داده و فرض توزیع نرمال، احتمال پیش آمدن یک وضعیت خاص در پایگاه داده را تخمین می‌زند.

- ✓ خطرپذیری مارکتر[3]

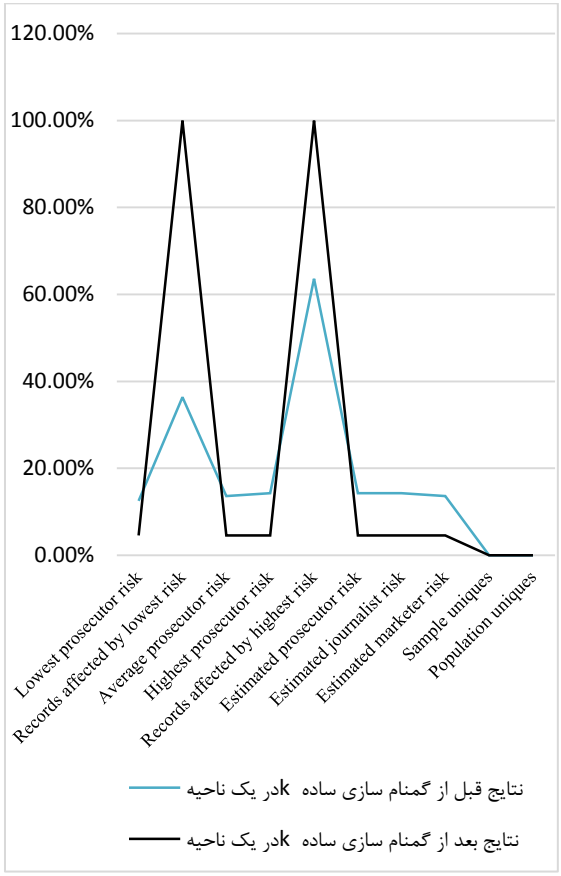
از احتمال تطبیق رکورد در یک کلاس هم‌ارز از مجموعه قابل‌شناسایی و مجموعه گمنام، اندازه‌گیری می‌شود.

دستاوردهای محاسبه خطرپذیری شکست حریم خصوصی به ترتیب، پیش و پس از اجرای الگوریتم گمنام‌سازی در شکل (۷) به نمایش گذاشته شده است. روش پیشنهادی، برای توسعه الگوریتم گمنام‌سازی در شبکه اقتضایی خودرویی، از ناحیه‌بندی خودروها بر پایه سرعت، راستای حرکت و جایگاه مکانی بهره می‌برد.



شکل (۷): مقایسه خطرپذیری پیش و پس از گمنام‌سازی

دستاوردهای شبیه‌سازی گمنامی k ساده در شکل (۷) ارائه شده و گویای کاهش مناسب خطرپذیری‌های تعقیب‌کننده، ژورنالیست و مارکتر است. هرچند کاهشی مناسب به‌دست‌آمده است، باید توجه داشت، در شبکه اقتضائی خودرویی توانایی پیاده‌سازی گمنامی فراگیر وجود ندارد؛ بنابراین، عملیاتی بودن الگوریتم را به چالش کشیده شده و به‌ناچار، نیازمند دسته‌بندی هدفمند خودروها، متناسب با پیکربندی شبکه است تا توانایی مقیاس‌پذیری الگوریتم فراهم شود.



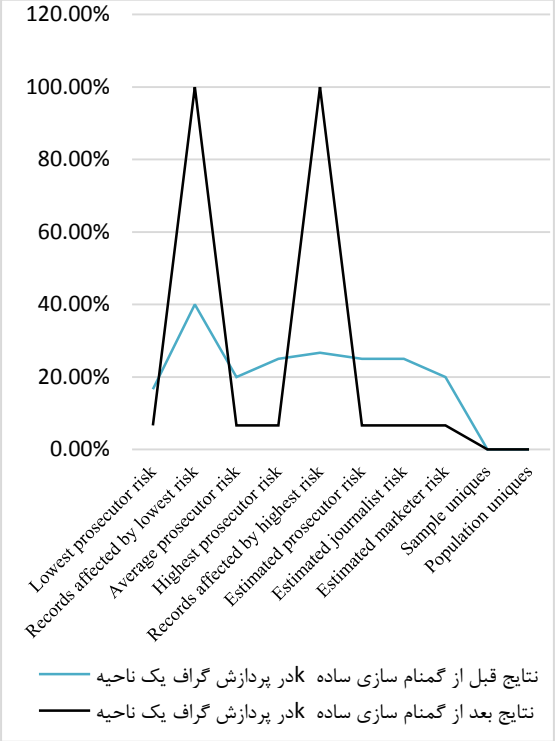
شکل (۸): خطرپذیری گمنام‌سازی در ناحیه شباهت

اکنون پس از اجرای الگوریتم گمنام‌سازی در ناحیه شباهت، میزان خطرپذیری شکست حریم خصوصی، برآورد و در شکل (۸) ارائه شده است.

در گمنامی k خودروها در گروه‌های دست‌کم k- تایی دسته‌بندی خواهند شد. خودروها در رئوس گراف گمنامی قرار دارند. آمیختن ویژگی‌های شبه شناسه، یال‌های گراف گمنامی را سازمان می‌دهد.

عملیات حذف و اضافه در گراف، بر پایه کمترین افزایش، کاهش و جابه‌جایی گراف، درجه گمنامی گراف را افزایش می‌دهد. برای ایجاد ابهام از روش افزودن گره ساختگی و برای ایجاد اعوجاج درداده، از حذف و تغییر ویژگی استفاده می‌شود.

[1] Prosecutor Risk
[2] Journalist Risk
[3] Marketer Risk



شکل (۹): خطرپذیری گمنام‌سازی گراف گمنامی ناحیه

اکنون با شبیه‌سازی الگوریتم پردازش گراف در گمنام‌سازی ناحیه شباهت، میزان خطرپذیری شکست حریم خصوصی برآورد و در شکل (۹) به نمایش گذاشته شده است.

۶- نتیجه‌گیری

آرمان روش پیشنهادی، گمنام‌سازی شبکه اقتضایی خودرویی است. این مهم با رویکرد ترافیک پرشتاب خودروها، با چالش‌هایی همچون سربار انبوه و شکست‌های فراوان هم‌بندی شبکه روبرو است. دستاورد پیاده‌سازی زنجیره بلوک، برطرف شدن چالش هم‌بندی است، در عوض، چالش تأخیر و سربار راه‌اندازی فرایند بسیار جدی است. روش پیشنهادی با سوار نمودن زنجیره بلوک بر شبکه اقتضایی خودرویی و به‌کارگیری رمزنگاری نامتقارن، گمنامی هویت و با جمع‌آوری تراکنش‌های کاربران مختلف در یک بلوک، گمنامی مسیر را تأمین و همچنین پایداری، کاهش مطلوب سربار و تأخیر اولیه فرایند را موجب می‌شود. از سوی دیگر، پیش از جمع‌آوری تراکنش‌ها در یک بلوک، با گمنام‌سازی گراف شبکه و فرایندهای سه‌گانه گره ساختگی، دوره خاموش و گمنامی k، امنیت تراکنش‌هایی که هنوز واگذار به فرایند زنجیره بلوک نشده‌اند، تأمین و خطرپذیری شکست حریم خصوصی را مدیریت می‌کند. به‌طور خلاصه، ارسال بلوک‌های مجتمع، سربار انبوه و توزیع‌شدگی داده در فرایند زنجیره بلوک، شکست‌های فراوان هم‌بندی شبکه را حل کرده است. دستاوردهای شبیه‌سازی گویای پایدار بودن زنجیره بلوک و کاهش مطلوب خطرپذیری و از همه برجسته‌تر، حل چالش سربار و تأخیر زیاد راه‌اندازی فرایند زنجیره بلوک معمولی است. روش پیشنهادی افزون بر به‌کارگیری گراف محلی در ناحیه‌های کوچک، به خودرو اجازه می‌دهد مدیریت حریم خصوصی خود را به‌دست گیرد. با تجمیع همه گراف‌های گمنامی محلی، می‌توان گراف گمنامی سرتاسری شبکه را پدید آورد و از مزیت گراف سرتاسری متمرکز بهره برد.

۷- مراجع

[1] B. Zhou, J. Pei, and W. Luk, “A brief survey on anonymization techniques for privacy preserving publishing of social network data,” ACM Sigkdd Explor. Newsl., vol. 10, no. 2, pp. 12–22, 2008.

[2] P. Shi, L. Xiong, and B. Fung, “Anonymizing data with quasi-sensitive attribute values,” in Proceedings of the 19th ACM international conference on Information and knowledge management, pp. 1389–1392, 2010.

[3] S. Zakhary and A. Benslimane, “On location-privacy in opportunistic mobile networks, a survey,” J. Netw. Comput. Appl., vol. 103, pp. 157–170, 2018.

[4] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, “Traffic-aware multiple mix zone placement for protecting location privacy,” in INFOCOM, 2012 Proceedings IEEE, pp. 972–980, 2012.

[5] K. Miura and F. Sato, “Evaluation of a hybrid method of user location anonymization,” in Proceedings 8th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA, pp. 191–198, 2013.

[6] R. Al-Dhubhani and J. M. Cazalas, “An adaptive geo-indistinguishability mechanism for continuous LBS queries,” Wirel. Networks, pp. 1–19, 2017.

[7] A. K. Tyagi and N. Sreenath, “Location privacy preserving techniques for location based services over road networks,” in International Conference on Communications and Signal Processing (ICCSP), pp. 1319–1326, 2015.

[8] I. Memon, L. Chen, Q. A. Arain, H. Memon, and G. Chen, “Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks,” Int. J. Commun. Syst., vol. 31, no. 1, 2018.

[9] Arain Qasim Ali, Zhongliang Deng, Memon Imran, Arain Salman, Shaikh Faisal Kareem, Zubedi Asma, Unar Mukhtiar Ali Ashraf Aisha, Shaikh Roshan, “Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks,” Wirel. Pers. Commun., vol. 95, no. 2, pp. 505–521, 2017.

[10] G. P. Corser, A. Banihani, J. Cox, R. Hoque, H. Fu, and Y. Zhu, “Location Privacy, Application Overhead and Congestion in VANET Location Based Services,” in Big Data Security on Cloud

[22] L. Baird, M. Harmon, and P. Madsen, "Hedera: A Governing Council & Public Hashgraph Network," 2018.

[23] L. Baird, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance," Swirlds, Inc. Tech. Rep. SWIRLDS-TR-2016, vol. 1, 2016.

[24] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, pp. 137–140, 2016.

[25] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, 2017.

[26] S. Rowan, M. Clear, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels," arXiv preprint arXiv:1704.02553. eprint.

[27] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," arXiv Prepr. arXiv1708.09721, 2017.

[28] S. M. Pournaghi, M. Barmshoori, and M. Gardeshi, "An Improved Authentication Scheme with Conditional Privacy Preserving in VANETs," J. Electron. CYBER Def., vol. 3, no. 2, pp. 1–12, 2015.

[29] Li Lun, Liu Jiqiang, Cheng Lichen, Qiu Shuo, Wang Wei, Zhang Xiangliang, Zhang, Zonghua, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 7, pp. 2204–2220, 2018.

[30] M. Yuan, L. Chen, S. Y. Philip, and T. Yu, "Protecting sensitive labels in social network data anonymization," IEEE Trans. Knowl. Data Eng., vol. 25, no. 3, pp. 633–647, 2013.

[31] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," technical report, SRI International, 1998.

[32] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, pp. 106–115, 2007.

[33] Wang Xu, Zha Xuan, Ni Wei, Liu Ren Ping, Guo Y Jay, Niu Xinxin, Zheng Kangfeng, "Survey on blockchain for Internet of Things," Comput. Commun., 2019.

(BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2017 IEEE 3rd International Conference on, pp. 243–248, 2017.

[11] P. Mahapatra and A. Naveena, "Enhancing Identity Based Batch Verification Scheme for Security and Privacy in VANET," in Advance Computing Conference (IACC), 2017 IEEE 7th International, pp. 391–396, 2017.

[12] A. Arora, N. Rakesh, and K. K. Mishra, "Analysis of Safety Applications in VANET for LTE Based Network," in Networking Communication and Data Knowledge Engineering, Springer, pp. 141–154, 2018.

[13] K. Logeshwari and L. Lakshmanan, "Authenticated anonymous secure on demand routing protocol in VANET (Vehicular adhoc network)," in Information Communication and Embedded Systems (ICICES), 2017 International Conference on, pp. 1–7, 2017.

[14] C. Zuo, K. Liang, Z. L. Jiang, J. Shao, and J. Fang, "Cost-effective privacy-preserving vehicular urban sensing system," Pers. Ubiquitous Comput., vol. 21, no. 5, pp. 893–901, 2017.

[15] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," IEEE Access, vol. 6, pp. 45655–45664, 2018.

[16] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new-type of blockchain for secure message exchange in VANET," Digit. Commun. Networks, 2019.

[17] S. Alboaie, D. Cosovan, L.-D. Chiorean, and M. F. Vaida, "Lamport n-time signature scheme," in 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), pp. 1–6, 2018.

[18] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in Conference on the Theory and Application of Cryptography, pp. 437–455, 1990.

[19] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in Sequences II, Springer, pp. 329–334, 1993.

[20] A. Kiayias and A. Mitrofanova, "Financial Cryptography and Data Security," Lect. Notes Comput. Sci., vol. 3570, pp. 109–124, 2005.

[21] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in Proceedings of the Future Technologies Conference, pp. 1037–1058, 2018.

Journal of Electronical & Cyber Defence
Vol. 8, No. 4, 2021, Serial No. 32

Distributed Anonymity Based On the Integrated Block Chain in Vehicular Ad Hoc Network

F. Rezazadeh, M. Agha Sarram*, K. Mizanian, S. A. Mostafavi
*Department of Computer Engineering Yazd University Yazd, Iran

(Received: 30/09/2019, Accepted: 01/02/2020)

ABSTRACT

The network overhead and multiple networks disconnection faults are the main challenges of anonymous servers implemented in VANETs. The block chain technology has been entered into the wide range of preserving privacy. The robust anonymity mechanism existence and the traceability of all transactions are the main advantages of this technology. The primary model of the block chain was able to complete the process with the anonymity stored data. In distributed models, the authentication, storage and retrieval of transactions are applied by all user's consensus. The asymmetric cryptography, preserves the identity anonymity and aggregating transactions of different users into a block which is ready to send, preserves the path anonymity. The proposed method is aimed to ensure anonymity by mounting the block chain on VANETs. Before delivering any transaction to the block chain, the risk of user's privacy is high. To achieve low risk, we combine the graph processing methods with Silent Period, Cloaking-Region and Dummy Node methods. The block chain simulation on VANET is driven by python and the anonymity risks are simulated with ARX. The results suggest that the block chain is stabled and the optimal risk reduction is achieved on the VANET.

Keywords: Block-Chain, VANET, Security, Anonymity, Cryptography

* Corresponding Author Email: mehdi.sarram@yazd.ac.ir